ICANN69 | Virtual Annual General – At-Large Policy Session: Coordinating the Internet Unique Identifiers and the Interests of the Internet Users
Monday, October 19, 2020 – 12:30 to 14:00 CEST

YESIM NAZLAR: Hello. Welcome to the Coordinating the Internet Unique Identifiers and the Interests of the Internet Users.

Interpretation for this session will include French and Spanish languages and will be conducted using both Zoom and a remote simultaneous interpretation platform remote simultaneous interpretation platform operated by Congress Rental Network. Attendees are encouraged to download the Congress Rental Network app following instructions in the Zoom chat or from the meeting details document available on the meeting website page.

If you wish to speak, please raise your hand in the Zoom room. Once the session facilitator calls upon your name, you may unmute yourself. Please state your name for the record and the language you will speak if speaking a language other than English.

When speaking, be sure to mute all other devices including the Congress Rental Network application. Please also speak clearly and at a reasonable pace to allow for accurate interpretation.

Finally, this session, like all other ICANN activities, is governed by the ICANN expected standards of behavior. Please find the link in the chat

for your reference. In the case of a disruption during the session, our technical support team will mute all participants.

With that, I will hand the floor over to Hadia Elminiawi. Over to you, Hadia. Thanks so much.

HADIA ELMINIAWI: Thank you so much. Hi, this is Hadia Elminiawi, ALAC delegate to the NomCom for the Africa region, leader of the DNS Entrepreneurship Center, and the moderator of this session.

Thank you again, all, for coming to At-Large Policy Session about Coordinating the Internet Unique Identifiers and the Interests of the Internet Users. Today, we are very lucky to have with us very special and distinguished speakers.

We shall first welcome Leon Sanchez, ICANN Board vice chair and At-Large elected ICANN Board director. Leon will talk to us about how coordination and collaboration between different stakeholders ensures policy development and technical functions are carried out in the public interest.

Following will be Dr. Steve Crocker, Internet pioneer, early ISOC and IETF leader, creator of [the] RFC [series], chair of ICANN's Security and Stability Advisory Committee from 2003-2010, and ICANN Board Chair from 2011-2017. Dr. Steve will discuss the interests of the Internet end users as they relate to the security and stability of the Internet.

Finally, I shall be talking about ICANN policy development and its impact on Internet end users. After that, we shall have 20 minutes for Q&A. So let's start.

Welcome, Leon. You have the floor.

LEON SANCHEZ: Thank you very much, Hadia, for inviting me to this session. It's always good to be back at home, as I always say when I participate on At-Large related sessions. So thank you very much. It's always also an honor to share a session with Steve. We do miss you, Steve, in the Board, and it's always good to share the floor with you.

Going to the topic and how coordination and collaboration between different stakeholders ensures that policy development and technical functions are carried out in the public interest, I think it's a topic that is not only interesting but also very complex.

Sorry, I am hearing some background noise. I think it's gone.

As I was saying, it's not only an interesting but also a very complex topic. Coordination amongst stakeholders, I think it's something that is at the very core of how the Internet works, how the Internet governance system works. It seems to be something that has happened since the very inception and since the very beginning of the Internet.

However, I think we need to ask ourselves some questions. What do we mean when we say stakeholders? Do we mean stakeholders within

the ICANN context? Do we mean stakeholders within a broader context? I think it is pertinent to think about the word or the meaning of stakeholders within a broader context and not only within the ICANN context.

An example of this may be GDPR. We know the effect that GDPR has had in the policies that govern the domain name system. Maybe if there had been some coordination amongst stakeholders before issuing the [law], the effects on the domain name system and its different policies would have been different. Maybe not lesser but at least taking into consideration the possible effects and the possible impacts that a regulation like the GDPR has had in the domain name system and other Internet related issues that have been impacted by GDPR.

So how do different stakeholders come into play when shaping policies that impact Internet end users? This is where I see value in broadening the scope for the definition of stakeholders. As I was saying in regard to GDPR, different policies are shaped of course within different contexts that may ultimately impact Internet end users. GDPR is just an example, but there are other examples of policies that are being shaped elsewhere that can impact Internet end users.

Let's say, for example, free trade agreements. We see how free trade agreements are incorporating some language that deals or intends to deal with ccTLDs and dispute resolution policies that are related to those ccTLDs. So this is a trend that I see growing in different trade

agreements that are now being negotiated by ICANN. I can tell you the USMCA and the European Union trade agreements between Mexico and the European Union also include this kind of language.

So if we don't coordinate with policymakers and with lawmakers when they are actually crafting these policies, the impact in the Internet ecosystem and of course the impact for Internet end users may not only be sometimes harmful but also entail some unintended consequences. This is why I think it is important that we coordinate in a broader context and not only within the ICANN context.

Now how can coordination be achieved? That's definitely a challenge because one of the things that I think we have been very careful while working in the ICANN community is trying to not politicize ICANN. We've seen how ICANN has gone through different phases, but the most recent phase that I can identify is one in which ICANN is trying to contribute to informed discussions while staying out or trying to stay out of politics. This is also a delicate balance that we need to take care of and we need to try to achieve. How can we [incite] in the shaping of public policies without politicizing ICANN?

This is where I think we need to get out of our silos and start talking to each other and try to find out what role do we as a community play in all this setup? How can we foster collaboration between stakeholders? The At-Large community, I think it's a key piece of this puzzle because through the ALSes that form the different RALOs and of course the At-Large community I think we have a very important and powerful tool

to reach policymakers at a local level and of course expand that local influence into a broader range in the international [inaudible] arena.

So I would like to leave you all with these thoughts in the table and of course listen to the other speakers. Because more than answers I think this session should be about fostering dialogue and trying to see how we can achieve this objective of coordinating amongst different stakeholders.

Thank you, Hadia. I would like to give the floor to you now. And of course I will remain in the session to continue discussing and am happy to receive any questions from the audience.

HADIA ELMINIAWI: Thank you so much, Leon. Indeed, a very interesting talk. I myself have some questions to you. But actually, we have 20 minutes in the end for Q&A, so let's take the questions in the end if it's fine with you, Leon.

LEON SANCHEZ: Absolutely, yes.

HADIA ELMINIAWI: Thank you so much. I would like now to move to our next part. Welcome, Steve. Great to have you with us today. The floor is yours.

STEVE CROCKER: Thank you very much. Can you hear me well enough?

HADIA ELMINIAWI: Yes, I can.

STEVE CROCKER: Okay, good. Thank you. Thank you, Hadia. And thank you, Leon, for your very kind words. It's indeed a pleasure to be back connected to the ICANN community, to ALAC in particular, and particularly with you, Leon. It was a pleasure working with you on the Board.

Leon, you raised some interesting questions which I want to address about the role of government policies versus ICANN policy development process in effect. I've been actually spending quite a lot of time on that from a different perspective which I'll come to at the end.

I'll focus for now on a presentation on security and stability issues related to the processes related to the unique identifiers of the Internet. And then I'll come back for some more direct response. I think I have to ask you to change the slide, so next slide, please.

That's a tiny bit of my background. We can skip over that. All right, the DNS ecosystem, this is a somewhat detailed slide, I want to focus your attention on the far left portion of it: the domain name registration process that has ICANN contracted parties, registries, and registrars. In the box that has the dashed lines around registrants are the parts that relate to the end users of the registration system. And then on the far

right, you have the end users of the Internet itself who are looking up domain name systems.

Of course what we all know is that domain names are at the very foundation of the way users and application programs use the Internet. We have a rather elaborate structure for creating domain names, registering them, administering them, and even paying for them. I assume everybody is relatively familiar. I would imagine a good fraction of the people on this call in this meeting have their own domain names or work for companies for which you're involved to some degree in administering them or that you are familiar with the processes in your organizations. Whether it's a government, a university, or a nonprofit or a for-profit company, everybody registers domain names and is very dependent upon them. Next slide, please.

I want to talk a lot about the security aspects. Security is a very broad term that encompasses a number of things. Next slide, please.

It's traditional to talk about three different aspects of security leading to what's traditionally called the CIA triad, a security model that helps people think about the various parts.

In reverse order from the initials:

Availability: ensuring data and services are available when they are required by their end users. This is absolutely important because if it's not available, then you can't use it and the rest doesn't matter.

Integrity: making sure that the data is accurate and has not been modified and that everybody can trust it. And then last but not least is:

Confidentiality: preventing the disclosure of the information to the wrong people either while that information is at rest, that is in storage, or is being transmitted along the transmission lines. Next slide, please.

With respect to the domain name system focusing on availability, we have at the very top of the domain name system the so-called root which is a list of all the top-level domains. That is provided on a worldwide basis through a set of name servers. There are 13 groups of name server. There are not just 13, but there are 13 constellations, I call them. The total number of servers is currently over 1,300 different machines placed strategically all over the world and that make it possible to retrieve the answer to the question, how do I reach the names associated with a particular top-level domain?

When your computer reaches out to say how do I reach www.ICANN.org, the system that it's asking about if there's no knowledge about that, a message is sent off to one of these root servers that comes back with a pointer to where you can find information about .org names. And then a subsequent query is sent to the .org name servers and so forth.

The second sub-bullet in there massively overprovisioned relates to this number that I just shared with you: over 1,300 separate name servers. This makes it possible to say with a great deal of assurance

that, first of all, these answers are always going to be available. Even if some of the machines are not working.

Or in the case that it happens more often than we'd like that there are massive attacks against the root servers, DDoS attacks, they still have plenty of capacity and are there to operate 7x24 around the world. And further that the responses come very quickly. That there are no real delays. This is really one of the truly magnificent parts of the Internet infrastructure.

The term "Internet" is coined as "a network or networks." This is extremely important because it permits individual operation of networks around the world. In each country, there could be one or more networks and often are. And these networks can be connected to each other in multiple ways. There's not just a single path between any two points.

One important element of the availability portion of the triad is that if one path fails, there's almost always another path available. The redundancy and the myriad of connections ensures that users can find services and resources they wish to connect with. This is always an evolving situation. As the network grows we have roughly half of the people in the world connected to the Internet. As we connect the other half, there will be many more connections. And even over time as the bandwidth increases and the number of computers increases, there will be more and more connections. Next slide, please.

Having all of the machines up and available is important, and the next portion of the story is, how can you trust that the data that you're getting is the accurate data that is intended for you? For this, cryptographic protocols that use modern cryptography are important. The focus on the cryptography is not—in this case, I'll get to it in a minute—on hiding the information but rather on making sure that the information you get is the information that you were intended to get.

There are secure protocols—SSL, TLS, HTTPS—that add cryptographic checksums and have keys associated with them so that the end user can check to see if the data that it receives is actually correct. This leads to the integrity of communication signals.

One very important part of this is the cryptographic assurance within the domain name system protocol. This is called DNSSEC which is the security extensions to DNS. This ensures that ensuing communications held between end users and intended resources are exactly what you want. I'll come back and emphasize some things about DNSSEC at the end. Next slide, please.

Finally, confidentiality. Users have a right to expect that the communications that they have either on a personal basis or even with services are private to themselves and are not spied on, if you will, by others. So that leads to the use of data encryption which scrambles the signal so that even if somebody is looking at it, they won't understand what is being said.

Built into SSL and TLS and HTTPS, which I mentioned before for integrity, is also the confidentiality aspect. And then more recently, we have new protocols. DNS over HTTPS and DNS over TLS that are recent technologies. Those are called DoH and DoT, sometimes pronounced "doe." Recent technologies that encrypt DNS queries themselves and protect the data in transit but not inside of the DNS servers. That has to be done in a different way. And then ISPs and software vendors make decisions on which technologies to adopt for their end users. Next slide, please.

That's the short story of availability, integrity, and confidentiality. Let me move on to the next slide and then talk about stability. Next slide, please.

We'll look a little more closely at the availability issues and we ask if the services delivered consistently and reliably. Here we have several different attributes. Do you get the same result every time? If you use a unique identifier, is there just one proper result? If you're using a resource you're working with, is it available everywhere on the network or at least where it is supposed to be? And then reliability and responsiveness. Can you access the data and services you need consistently? And do you get the desired interaction in sufficient time? These decisions on Internet protocols, identify policy, and provisioning services are made to achieve these goals for Internet end users. Next slide, please.

The naming system and the numbering system are uniquely assigned to ensure unambiguous and consistent results. ICANN, the ccTLDs,

and the domain name provisioning industry ensure the interoperation of all the domain names. The root DNS service provides a single consistent foundation worldwide for the top-level domains and individual names in the hierarchy.

There have been attempts to create alternative roots for other protocols and alternative roots for DNS. The alternative roots for DNS have largely failed. From an ICANN perspective and an Internet global perspective, alternative roots would have the effect of effectively splitting the Internet, and that we view as not a very good thing at all. Alternative roots for other protocols have a mixed history, and some of them are doing okay.

On the numbering side of things, we have five major organizations around the world called regional Internet registries. In Africa, AFRINIC. In Europe, RIPE NCC. In Latin America, LACNIC. In the Asia Pacific region, APNIC. And in the North American region, ARIN.

They administer the allocation of IP addresses and what are called autonomous system numbers that are used in the routing system. And then they make allocations to ISPs and other large organizations. And then hierarchically, those are distributed further down.

The ISPs themselves engage in the actual routing of data packets from one place to another, and they have rather elaborate peering and routing protocols that they use and exchange on a moment-by-moment basis to make sure that they know how to reach everybody on the Internet.

And then of course there is an underlying infrastructure of software developed by many organizations that uses the protocols that are developed within the Internet engineering task force. Next slide, please.

In order to make all this work, and everybody does expect that it just works, there are multiple things that are required. The overprovisioning and redundancy that I emphasized before are very important. And then structuring things so that there are many paths from one place to another. And then you have content delivery networks that are a reasonably modern, I guess not so new, but in any case relatively new in the life of the Internet—that move data closer to the users, distribute the loads, and provide much quicker and sometimes location dependent responses for the users. Next slide, please. And then the next slide again.

I'll close this part and simply come back and mention that DNSSEC is a very important portion of the story. We have maps that show how many of the top-level domains around the world have implemented DNSSEC. The answers are nearly 100% in Europe, 100% in North America. A very, very strong uptake in Latin America and in the Asia Pacific. And Africa is moving along, but there's a lot more work to do in Africa.

All of the generic top-level domains are signed, and that's a requirement under the ICANN contracts that deal with the generic top-level domains. The use of DNSSEC has two parts to it. One is that the domain names have to be signed, and that's the part I just spoke to,

and the other is that the signatures need to be checked. That's the validation side of it. That is not quite as far along as the signing, and so there's pressure that should be applied to increase the use of validation as well as some pressure to get DNSSEC to be adopted on the signing side.

With that, that's the end of the prepared remarks on this, and I look forward to questions. But I also want to say a few words related to the topic that Leon brought up about policy development and so forth.

I've been following the interaction, particularly related to GDPR, but more generally related to privacy regulations around the world. I've been following the development of WHOIS protocols and the policies related to them for a long time. The WHOIS protocols go back farther than you might imagine.

In the very earliest days even before we had an Internet, we had just the ARPANET. The machines that were connected to the ARPANET were so-called timeshared machines where several users used the same machine. The WHOIS protocol grew out of trying to list the system administrators who were running each of the timeshared machines and publishing their names so that they could reach each other. It had nothing to do at first with the end users. It only had to do with the system administrators.

Fast forward several decades and scale up by a factor of a million and nothing stays the same. The domain name system was created. A network of networks was connected. And now the WHOIS data

became used to find who the owners were of domain names as opposed to who the system administrators were of the timeshared systems.

This brought on a number of secondary issues of accuracy and of privacy and misuse of this information and many attempts repeated over many years to try to build new policies. The interaction of the government regulations, particularly GDPR, caused a somewhat abrupt, more abrupt than necessary perhaps, but an abrupt swing over toward privacy issues as opposed to the utility or accuracy and has shut off access to a lot of that data.

From a privacy point of view that I suppose is viewed as a good thing. But from an overall system perspective it's a very crude, not very nuanced, and not very deeply thought through kind of situation. And then, as Leon suggested, it would be much better if there were more detailed kinds of interactions and the ability to think through what the consequences are.

I will suggest that, though it's certainly useful to engage in interactions with governments and to try to do so in an objective and nonpolitical way, I would also suggest that we could also look inward at the ICANN policy development processes.

In my view—and this is I want to say very strongly that I'm speaking myself based on experience of course but nonetheless not speaking for ICANN or any other organization—but in my view ICANN and the whole ICANN community could be doing a much deeper job of looking

at the issues, studying them in advance. And prior to entering the sometimes heated negotiation sessions in the policy development process do quite a bit more homework on what the alternatives are and what the real issues are as opposed to some extraneous ones.

And also to demand that everybody be speaking the same language. I've observed that there's a lot of speaking past each other or trying to avoid reaching consensus because it serves one party but not the others.

So those are my somewhat provocative comments on that. And with that, I turn the floor back over to you, Hadia, and I'm more than happy to engage in discussion.

HADIA ELMINIAWI: Thank you so much, Steve. Indeed, this is a very important discussion. Let me go through my part quickly, and then we'll have definitely more time for discussion than those 20 minutes for sure. We shall try to target about 35-40 minutes. If I could have, yes, the next slide, please.

I shall be talking about the impact of ICANN policies on end users. First, I'll start with an introduction and then we'll talk about how ICANN develops policies and who determines what policies need to be developed. And then I shall give some examples of ICANN policies' impact on end users. If we could go to the next slide, please. Thank you.

The At-Large Advisory Committee gives the opportunity to any individual no matter his or her background to participate in the unique identifiers policymaking process. The reason for having a committee dedicated to end users is that ICANN policies do not only affect the technical community or Internet related businesses but also primarily affect Internet end users whom the Internet ultimately serves. Could we have the next slide, please?

How does ICANN develop policies? More importantly, who determines what policies need to be developed? Policy recommendations specific to gTLDs per ICANN bylaws are developed through the GNSO policy development process. While cross-community working groups allow for any number of supporting organizations and advisory committees to work together to address issues of common interest that do not fall within the sole remit of one supporting organization or advisory committee. Internet end users through their involvement and engagement with the At-Large community do not only provide advice in relation to ICANN policies but also participate in policy development.

Whenever ALAC realizes that a policy is of interest to end users it enlists interested At-Large members to the ICANN working group developing the policy. Examples to that include the application support program for new gTLDs and the auction proceeds.

Not all superheroes wear capes, and Internet users, you are the superheroes. As the end users interests are an integral part of ICANN policy development, in the following slides I shall show some

examples of current ICANN PDPs and cross-community working groups and show how their outcomes may affect end users. I have tried to focus on current and recently developed policies, but I will mention some ancient ones as well. Could we have the next slide, please?

The first example I have here is the new gTLD auction proceeds. This is an example of a cross-community working group that was chartered by all ICANN supporting organizations and advisory committees for the multistakeholder groups to reach consensus on a plan to use the money of the new gTLD auction proceeds. The objective is to use the money in accordance with ICANN's mission to the benefit of the Internet community.

The projects funded by this money are expected to contribute to addressing diversity, inclusion, and [inaudible] participation among other things. This gives end users wider opportunities to engage and participate in ICANN policymaking. It also empowers Internet users by giving them a role in the Internet policymaking process. If we could have the next slide, please.

The next policy I am bringing up is the expedited policy development process on gTLD registration data. This is an example of how new legislation may affect current implemented ICANN policies and subsequently how this affects Internet users. gTLD registration data could previously be created through a system called WHOIS which would provide data in relation to a registered domain name, such as the name and the contact information.

With new privacy legislation, WHOIS as we used to know is no longer possible. The new laws enhance the registrant's privacy but affected the security of the domains and that of the online users. The EPDP on gTLD registration data tries to find a balance between the privacy of the registrants and the legal requirements versus the security and stability of the domains as well as the safety of the Internet users.

Verifying the legitimacy of a website and tracking DNS abusers was the main purpose for accessing registration data. We have all seen with the current pandemic how people around the globe are depending on the Internet in almost every aspect of their lives. Whether it is working from home, learning from home, shopping, accessing various services such as medical and government portals, or looking for information and seeking resources, the legitimacy and security of the domain names is crucial. To that end, the impact of such a policy on Internet users is inevitable. Could we have the next slide, please?

The next policy I will mention is the new gTLD subsequent procedures. This policy prepares for possible new rounds for new gTLDs, and this ultimately should give room to community TLDs and internationalized domain names. Supporting a diverse pool of applicants should create an impact on local communities and thus the Internet users.

Another thing I would bring up here is though it's not a policy development process per se it's an ICANN supported community initiative. Again, it's not a policy development process, however I thought its impact on end users is worth mentioning. This is the

universal acceptance steering group which is an ICANN supported community initiative.

The UASG works on the universal acceptance of all ACSII domain names, ACSII email addresses, IDN domain names, and IDN emails. The impact of this on end users is certain where they would be able to access websites entirely in their own languages as well as use email addresses and [inaudible] in their local languages. Moreover, all ACSII domain names would be treated equally allowing for a consistent user experience across all domain names. Just to note, of course there are a lot of ICANN IDN related policy developments, such as those in relation to Label Generation Rule 6. Could we have the next slide, please?

I will try here to touch on ICANN policy and DNS abuse. Again, this is a very important issue when it comes to Internet end users and also when it comes to the expansion of the domain space. So one of ICANN's oldest policies is the uniform dispute resolution policy which was developed to address the issue of cybersquatting. The policy provides a fast track arbitration process giving a path for domain owners to recover their domain names without the need to go to court.

Add grace period limits policy is another example of a GNSO policy that also addresses a form of DNS abuse. [inaudible] is also a good example of the bottom-up consensus-driven process where the user community at large played a role in bringing attention to the issue

which was addressed by a GNSO PDP. This stopped an abusive domain name behavior that exploited the five-day add grace period.

Such policies as well as registration data policies have a role in mitigating DNS abuse and helping cybersecurity professionals in addressing DNS abuse actions thus protecting Internet end users from criminal and/or harmful acts. If we could have the next slide, please. And this is where I conclude.

ICANN developed policies are developed by the community through a bottom-up consensus policy to serve the entire Internet community ensuring the security and stability of the unique identifiers and subsequently ensuring Internet users have a reliable, safe, and secure online experience. The ultimate beneficiaries of the Internet policies are actually the Internet users.

With this, I finish and thank you. Let's move to the Q&A session. We have about 40 minutes for that. please, if you have a question, raise your hand. I have a question that was in the chat from Sivasubramanian, and it's to Steve. The question is: "Is there some way by which a choice of essential technologies are standardized between ISPs and others?" Steve, if you are talking, we cannot hear you.

STEVE CROCKER: Okay, can you hear me now?

HADIA ELMINIAWI: Yes, thank you.

STEVE CROCKER: Good. The choice of technologies that ISPs use is governed fundamentally by market forces. This is one of the more unusual and important aspects of the way the Internet is constructed and is sometimes hard to understand and sometimes causes some confusion.

Unlike the telephone systems of the old days, the standards that are used are not imposed from the top down by governments. Instead, protocols are developed and standardized through the Internet Engineering Task Force. But the standardization process very carefully separates the agreements on what the protocols should look like as opposed to whether or not you have to use those protocols. That's determined by what I said is market forces. So individual vendors in designing their products and individual ISPs in designing their systems choose which protocols to adopt.

Now anybody who chooses not to use some important finds themselves in a very disadvantaged position. So the market forces are very, very strong and have the desired effect usually of moving things in the direction of everybody using common protocols. But the adoption process is not driven by regulation. It's instead, as I said, driven by choices made by the individual participants, by the vendors on the product side and by the ISPs and service providers in general on the service side.

As I said, this is sometimes a concept that is unusual from the perspective of people who've grown up in a highly regulated environment, and particularly governments that are used to regulating the telephone system.

So I think that's the answer, Shiva, that you may like or you don't have to like it. But that is the way it has worked. And I have to say it has had enormous success. It is one of the things that has led to the Internet growing as rapidly as it has and allowing creativity to come in. So you have development of new protocols. You do not have a heavyweight bureaucratic process that tends to inhibit the creation of new technologies. You have instead market forces that balance out the costs versus the utility of these things.

HADIA ELMINIAWI: Thank you so much, Steve. Actually, I have two questions for you and I have one for Leon. I see Marita Moll's hand is up, so I will take her question first. Marita, you can take the floor.

MARITA MOLL: Thanks, Hadia. My question is, well, it was Leon that piqued my interest here when he said something about trade agreements. Many years ago at the beginning of the North American Free Trade Act I used to keep track of that stuff, mostly on the issues of data sovereignty. I'm wondering—Leon, I think this might be your area of expertise—can you give us a real example about how the trade agreements could be or where they're going to be relative to ICANN's mission? Thank you.

LEON SANCHEZ: Thank you, Marita. Yes. In essence, I've seen some trade agreements evolve and how they're been negotiated. I can speak about particularly two processes. You might remember ACTA which is a trade agreement that encompasses the whole Asia Pacific region. And also the USMCA, the successor of NAFTA.

You can see how the language evolved from ACTA to the USMCA in which when ACTA was negotiated they included some language along the lines of having the involved parties or the involved countries signing ACTA to include provisions that would allow trademark holders to resolve disputes in their locally assigned top-level domains. That means ccTLDs. When they included that language, they included language that said that those dispute resolution policies would need to be in line with ICANN's dispute resolution policies. That was the language that was inserted in ACTA.

When you see the language that was inserted in USMCA it deletes the reference to ICANN dispute policies from the text. It still speaks about the countries involved needing to have dispute resolution policies that would of course encompass their ccTLDs when it came to dispute resolutions. But the reference to the ICANN dispute resolution has been deleted.

So my feeling is that if those trade agreements don't make the reference to ICANN dispute resolution policies, then we might begin seeing how policy dispute resolutions at a local level might deviate

from this GDPR and it would in the future eventually create some challenges in the space of dispute resolution and domain names. But that's just me speculating. I'm not saying that this will happen and that we will be seeing chaos in the near future. But I'm pretty confident that our lawmakers are specialists in creating chaos, so that's why I fear we should reach out in a more proactive way to try to inform their policymaking processes and try to warn them about unintended consequences that their policies might create in [status] other than the public policy itself.

MARITA MOLL: That's extremely interesting, Leon. Thank you very much. It's worth following.

LEON SANCHEZ: Thank you, Marita.

HADIA ELMINIAWI: Thank you, Leon. I have a hand from Sebastien, but I will quickly ask one question and then leave the floor to Sebastien. My question is actually to Leon. So, actually, Leon, you were talking about a framework. You were talking about coordinating with policymakers and lawmakers. [Going] to talk to them and contribute to the discussions while staying out of policy. Also, I very much liked what Steve said in relation to this and that it is very important also to look

within the ICANN community and look for solutions to the issues that we have.

But my question to you is in relation to what framework can we actually work through in order to have those discussions with policymakers or lawmakers? Who will identify who to work with or talk to, and who will be doing the talking? How can we have a framework within ICANN to actually do that? Because I'm not sure how acting individually in relation to this can actually result in actually effective results that would contribute to the making of the laws or policies.

LEON SANCHEZ: Thank you, Hadia. If I understood your question right, you're asking me how we as communities should guide this engagement with policymakers to try to engage. Is that correct?

HADIA ELMINIAWI: Should we have a framework for doing this? How do we as a community go ahead and make those discussions in order for those discussions actually to have an impact? Should there be a framework for that to start with?

LEON SANCHEZ: I'm not sure we can set up a framework for our community to engage in these kinds of discussions. When you think about engaging with policymakers and lawmakers from the ICANN perspective I think it's clear to me that it is ICANN Org who engages in that dialogue and the

one who has the ability to speak on behalf of ICANN as an organization.

When it comes to community members or parts of the community engaging in this dialogue, then that's a different issue. That's a different question. I don't think we as a community would be able to say, okay, you can reach out to policymakers or lawmakers as long as you follow this framework because in the end every part of our community is independent and has its own rules, its own processes, its own methods.

So I think in this issue the Internet governance engagement group, the IGEG, is a good tool for us to coordinate amongst us as a community and try to establish these guidelines or this framework that you're talking about so that when we go out of the ICANN bubble and try to engage with the outside world we are able to follow these guidelines or this framework that have set up from within the community.

But I wouldn't think of this framework as something that would be hard coded into our community colleagues but instead just as guidelines for engagement maybe. I hope that answers your question, Hadia.

HADIA ELMINIAWI: Thank you so much, Leon. I go to Sebastien. Please take the floor.

SEBASTIEN BACHOLLET: Thank you very much, Hadia. Thank you for setting up this conference or discussion. That's great that we have some time to discuss.

I was tempted to do it in French, but I don't want to bother our colleague and particularly Steve with my French. I will try with my English. I am very happy that you are back, Steve, my best chair on the Board. And, Leon, also it's good to have you participating to our discussion.

I wanted to raise two issues. The first one is that when, Leon, you talk about multistakeholder inside and outside of ICANN, I am sure that one way you are thinking about and we need to think about is how we can evolve ICANN multistakeholder to [imbed] those people within ICANN and not to leave them outside of ICANN.

I really consider that the discussion we had this morning with the Board regarding the evolution of the multistakeholder model including the proposal made by ATRT3 about holistic review must be one way to try to go and not just to leave them outside and to see how we can bring them inside.

The second comment/question is that there are new words coming around Internet. It's law, regulation, and sovereignty, and digital sovereignty more particularly. How does it fit with the multistakeholder model once and with the Internet more globally? Because if as you described it, Steve, Internet was not built to be something for one country or for one group of people but really to be open to the world. Thank you very much.

HADIA ELMINIAWI: Thank you, Sebastien. Steve or Leon, do you want to comment?

STEVE CROCKER: First of all, it's a real pleasure to see and hear you, Sebastien, and particularly to see how productive you've been with your beard.

I'm not sure what to add in a very deep and substantive way. The involvement of ALAC and the members of ALAC [and] the end users of the Internet I think is absolutely vital. It's a complicated process.

I come from basically a scientific and engineering background, so I tend to look at the ICANN ecosystem in terms of we built sort of a machine and is it working the way we want. So in order to diagnose Any problems that are in there or how to make improvements even if it's working pretty well one has to go and understand how old the different parts interact with each other and what are the underlying principles. That's why I often emphasize understanding a deep dive into the subject matter and looking closely at both what are the possibilities and what are the limitations whenever there is a desire to make a change or to set a policy.

It's hard for end users to engage in that unless they're also deeply knowledgeable about all of the inner workings on the technical side and the bureaucratic and political side. But as an organization, ALAC has the advantage of enormous breadth, global breadth, and touching

every element of society and the ability to draw on expertise from different areas.

So I think if the dialogue within ALAC is along those lines and then it engages in attempts to—sort of, how do you fix the machine or how do you diagnose what the issues are or how do you set goals that are consistent with what's possible.

I want to emphasize that last point about what's possible. I have watched over the years policy development processes that have committed two kinds of errors that are in the opposite direction. Sometimes there are people who argue vigorously with each other with the assumption that only one of them can succeed, a sort of zero-sum situation, when it's sometimes possible to do better so that more possibilities exist than they are assuming. And then of course on the other side a very common problem in all of human endeavors is people sometimes want more things than are possible. So it's important to understand both the possibilities that are available and the limitations that are inescapable.

HADIA ELMINIAWI: Thank you so much, Steve. Yes, indeed, setting goals that focus on what is possible is very important. You mentioned the ecosystem. I would like to bring you back to the ecosystem diagram if maybe staff could have this on the screen because it actually relates. Yeah, before that. It's I think the second or third slide maybe.

YESIM NAZLAR: Hadia, do you mean your presentation?

HADIA ELMINIAWI: No, I mean Steve's presentation. The DNS ecosystem.

STEVE CROCKER: Slide Number 3. This one I think is what you're talking about.

HADIA ELMINIAWI: Yes. This is actually a very interesting slide because it highlights the four key elements of the ecosystem. My question to you, Steve, is if possible if you could highlight the best practices in relation to each of the key blocks. For example, the content delivery, the content hosting and services blocks. What are the best practices in relation to each?

STEVE CROCKER: That's a very interesting question, and thank you very much for that. There's an awful lot to give you a complete answer, and I'm not even sure that I know all of the details. So I'll say a few things and then leave the rest for later.

But first of all, I'm glad that you've come back to this slide. It allows me to give a shout out to Steve Sheng on the ICANN staff and in general to the ICANN staff. This is a part of the product that comes out of the ICANN staff, and I think that they don't get enough recognition or appreciation for the work that they do.

On the content delivery side, so you're talking about the box. I don't think I have a pointer here that I can use usefully, but we're talking about the box on the bottom: content hosting and services. And then within that, you see five examples: web hosting provider, web servers, content delivery networks, mail hosting providers, and mail servers.

Each of those represent in a way a little industry or in some cases a big industry that has evolved over the years of the Internet. And within each of those areas they have their own best practices sometimes reached by agreement and sometimes learned the hard way when things don't work.

I'm just going to try to name one or two specifics without trying to go into everything. Content delivery networks are, as I had mentioned earlier, a relatively recent at least in the life of the Internet phenomena of moving content, making copies of content, and putting it in different places around the world so as to make it faster and cheaper to deliver that content to the people who want it.

In the process of doing that you also get some local variations. So what might be delivered on one continent may be different, partly to serve the differences in languages and so forth. But there are also political considerations that come in at that point. So you get some very delicate interplay between trying to be efficient about delivering the same content to everybody versus the much more nuanced and sometimes troubled issue of, do you make changes because it's helpful to the end users or do you make changes because it's helpful to the governments or other bodies that are involved?

So the best practices that developed are sometimes explicit and sometimes private matters or not very well discussed. I think a very important role for ALAC would be to ask the hard questions and gather data to the extent that you're in a position to do that about what the service looks like.

I just picked content delivery networks as a single example, not to say that they have problems that the others don't. Every one of these areas has issues. On the mail side, we frequently find that mail is rejected from certain sources because the servers are blacklisted. And that leads to questions of proper use and whether or not [improperly] or whether or not there is a way to undo unfair listings like that.

So I'll just stop there. I'm happy to talk about any other part of this that you wish.

HADIA ELMINIAWI: Thank you, Steve. Of course highlighting also the best practices in relation to other parts. However, being conscious about the time and we have some hands up, I would like to give the floor to Matthias. And if we have time, we can go back to my question and maybe some others as well. Matthias, please take the floor.

MATTHIAS HUDOBNIK: Hello. Can you hear me okay?

HADIA ELMINIAWI: Yes.

MATTHIAS HUDOBNIK: Great. Thanks a lot for this great session. I am really enjoying it. My question is for Steve. I would be curious to hear his opinion about DoH and DoT development and how this [evolve] related to our current DNS from a technical and a regulatory perspective also related to the IGF efforts. What are you thinking about the development? Thank you, Steve.

STEVE CROCKER: Well, thank you for the question. There are multiple things. The reason I'm pausing is because there are several thoughts that are coming into my mind at the same time. It has certainly been important to pay attention to how fast DoH and DoT have attracted attention and become adopted. So that indicates that there has been quite a lot of concern about protecting the privacy of queries.

For people who have not been following this, let me just describe the issue in very, very simple terms. If you can watch the sequence of queries and responses that are coming out of a particular organization or from a particular user, you can learn quite a bit about what they're interested in and that in effect is a serious invasion of their privacy. A slightly more subtle issue is the part of that that is most interesting is what the questions are, not what the answers are. What queries, what domain names are being looked up as opposed to what the answers are. The answers are generally public anyway.

So DoH and DoT are two very similar approaches for cloaking or hiding what the queries are while those queries are being transmitted. When they get to the server the resolve are that has to answer them you have to trust whether that resolver is also going to protect the information about who asked for which answers.

That's leading to a certain degree of consolidation a very high capacity resolvers that assert, that tell the world we are here to protect your queries and we won't share that information. But that aggregates the information and makes them subject to possible attack and raises the level of concern about how protected it really is. There's no data that suggests that that's not working as intended, but it is a concern that has been raised.

There are organizations both bad guys and law enforcement and other groups that have made quite a lot of use of watching the domain name queries and they are feeling unhappy that they can't see as much as they were saying before. So that then enters into very delicate public policy questions on the balance between privacy and law enforcement issues which I don't think there's any broad agreement on and both traditions and laws vary considerably around the world.

Is that helpful?

HADIA ELMINIAWI: Thank you, Steve. We have a question from [Shakri] in the chat, and then I will go to Yrjö. The question says, "By following Steve's

EN

intervention, I've got the impression that the coordination between stakeholder and ICANN [inaudible] is a technical issue and not a policy one. This somehow reflects the great impact of technical studies on ICANN policy development process. EPDP case is a good example. Do you think that these practices are healthy for PDP development?"

STEVE CROCKER: I'm having a little trouble understanding where the question is with respect to what the answer is. I'll just say, and here I'm quite opinionated about this and so I want to emphasize that these are my opinions and not necessarily everyone else's, I've watched the WHOIS and the registration data directory services as it's now called issues, the EPDP and so forth.

There's a lot of very, very serious earnest work that everybody has put into it and I don't want to diminish it in the slightest. At the same time, I genuinely believe that there's been a sense of urgency that has interfered with careful analysis of the alternatives and untangling the various issues.

I expect I will be making some quite serious presentations on this over the next several weeks as some work that we've been doing quietly for the last few years becomes visible. So I'll just leave it at that.

HADIA ELMINIAWI: Okay, thank you, Steve. So I think we are looking forward to seeing some of this work. Yrjö, I give the floor to Yrjö.

YRJÖ LÄNSIPURO: Thank you, Hadia. I'd like to thank Leon for pointing out the possible role of At-Large Structures (ALSes) in reaching out to policymakers in their respective countries. Now there's a good example in the chat from U.K. This happens in many other places too in many other countries, including mine.

The question is whether an ALS has standing, so to speak, for that sort of reaching out. I think that the more an ALS is involved in the multistakeholder Internet governance activities in their country the more standing, the more credibility they have to actually do that sort of reaching out. Thank you.

LEON SANCHEZ: Hadia, may I?

HADIA ELMINIAWI: Yes. Please, go ahead.

LEON SANCHEZ: Thank you. I completely agree with you, Yrjö. I think that also linking this to what Sebastien was saying about how we could incite in the shaping of public policies, I think that the saying that goes around saying act locally but think globally encompasses exactly this concept. We as ALSes can act at a local level but with a global conscience of the impact that our work can achieve.

And about standing, I think that you are exactly correct. The more one ALS participates at a local level with accurate information, with trusted information, with informed points of view, with information that can spread and that can share to the local community, the more respect that ALS will enjoy. And of course the more impact its participation will have.

So again, I think that we as At-Large community have solid gold in our community of ALSes and we should take advantage of that network of ALSes globally to help shape these public policies in the best interest of end users. So I think I completely agree with you, Yrjö, and we should definitely take advantage of our global network of ALSes. You are on mute, Hadia.

HADIA ELMINIAWI: Yes, thank you, Leon. I guess this is one of the next steps that we should be looking forward to as an At-Large community. Seeing no hands up, I have one related question to registration data to Steve. Steve, you actually applied the CIA triad model to the registration data in one of your slides. I don't know if we could have this on the screen. It was Slide Number 9.

In applying actually the model to the registration data when we look at the availability of the registration data what is needed for that is the protocol that actually replaces the WHOIS protocol, and that's the RDAP and that we have. And we need the system, a system for access/disclosure of data, and we do not have this yet.

And then looking at one other [fork] of the triad, the integrity, and this speaks to the accuracy of the registration data. Again, we are not—there is a great doubt about the accuracy of the data that we actually have.

And the third is the confidentiality, and you mentioned here the privacy and proxy services. And that part maybe we do have a complete service there.

So what are your thoughts in relation to those three elements and the registration data?

STEVE CROCKER: Thank you very much, Hadia, for the question. I'll take note of the fact that we are a couple of minutes before the end of the session. And so instead of my usual 30-60 minute answer to these questions, I'll try to condense it down.

RDAP is indeed an available protocol. RDAP by itself doesn't tell you what data is going to be requested, what data is going to be returned, and who should have access to it. It's a building block, a very important building block, but then you have to use it in a particular way. And that involves templates and policies and so forth.

SSAD is a proposed development by ICANN Org for providing unified access but unified access to the contracted parties data, to the gTLD information. One of the questions which might be of interest to ALAC

is, what about access to the ccTLD data? What about access to the RIR databases?

In the work that I've alluded to that we've been doing separately that I'll be announcing in a few weeks is to take a slightly larger picture and embracing the inclusion of all of these different parties and what the system implications would be.

On the accuracy, let me offer a somewhat provocative and slightly humorous perspective. There are a lot of complaints about the accuracy of WHOIS data. But if one stands back and looks at this completely fresh and says, "What is all this for?" when with registrant sets up an account with a registrar and provides the necessary information—credit card and other details—the two of them, the registrar and the registrant, do not have any problem about the accuracy of the information. If they registrant does not provide accurate information to the registrar, the registrar has very easy recourse. He simply stops providing service to the registrant.

So the complaints about accuracy are coming from other people— from law enforcement, form intellectual property attorneys, from domainers, from security researchers, and from others—who say they're not happy with that information. It's kind of amazing if you look at it from a different perspective that the information is as accurate as it is. One could have asked, why would anybody put any information in there unless you really want to be reached? So I think there is a kind of fresh look that's needed on the discussion of accuracy.

The security and stability advisory committee (SSAC) has actually laid out a hierarchy of validation levels from nothing at the base, take whatever information is provided, to the next level of it's got to look syntactically correct. So if a phone number is requested, it should look like a phone number instead of just a garbage or empty string. And then next level above that is it should be operational. So for example again for phone numbers, so that if you call it, it should get answered. And finally, a fourth level that is it actually has to match the intended purpose so that if you call that phone number, it gets answered by the person that you expect it to be answered by. Just to take the single example of phone numbers, but the same would be true of every other data element, and there are quite a few data elements involved.

So there are deeper discussions to be had about availability and [applicability] across the system on the one hand, about integrity of issues related to accuracy, and the confidentiality is where most of the major controversies are about who should have access to which data. And again, that's a much longer discussion but fortunately we've used up all the time so I don't have to speak to that.

HADIA ELMINIAWI: Thank you, Steve. Yes, our time is up. I thank you so much for this very interesting session. I thank you, Leon, as well very much for your very insightful talk and making us think about which stakeholders do we talk about and also how to engage with policymakers and lawmakers.

Going forward I have seen a lot of discussion in the chat about capacity building and indeed this is what we are doing. So there is a lot to build on, but our session is already ended. And I thank you all for your participation. I thank you, Steve, and I thank you, Leon, for being with us today. And I look forward for similar discussions. Thank you all.

STEVE CROCKER: Thank you for inviting me. It has been a very interesting session. You've done a fantastic job.

LEON SANCHEZ: Likewise. Thank you very much, Hadia. Thank you, Steve, and everyone for coming in and listening to us. Thank you.

[END OF TRANSCRIPTION]